Online Safety & IT Policy – October 2020

Rationale:

At Town Field Primary School, we feel it is important to teach pupils about the underpinning knowledge and behaviours that can help our pupils to navigate the online world safely and confidently regardless of the device, platform or app. Today's pupils are growing up in an increasingly complex world, living their lives seamlessly on and offline. This presents many positive and exciting opportunities, but also challenges and risks. Town Field Primary School equips pupils with the knowledge needed to make the best use of the internet and technology in a safe, considered and respectful way, so they are able to reap the benefits of the online world.

Our E Safety program of study complements the computing curriculum, which covers the principles of online safety at all key stages, with progression in the content to reflect the different and escalating risks that pupils face. This includes how to use technology safely, responsibly, respectfully and securely, and where to go for help and support when they have concerns about content or contact on the internet or other online technologies. Alongside this, our school builds in additional teaching as required to ensure our pupils are receiving a fully rounded education with regards to online safety both in terms of how to stay safe but also how to behave online. Our school's internet provider operates a filtering system that restricts access to inappropriate materials.

1. Aims and Objectives:

1.1 This policy relates to and should be read alongside other schools policies including those relating to Behaviour and Anti-Bullying, Safeguarding and Child Protection, the PREVENT agenda, Data Protection, GDPR and the Safe Use of Images.

1.2 This Online Safety and IT policy aims to:

- Allow young people to develop their own protection strategies for when adults set clear expectations of behaviour and/or codes of practice relevant to responsible use of the internet for educational, personal or recreational use
- Have clear structures to deal with online abuse, such as online bullying, which are cross referenced with other school policies
- Ensure that all members of the school community are aware that unlawful or unsafe behaviour is unacceptable and that, where appropriate, disciplinary or legal action will be taken
- Minimise the risk of misplaced or malicious allegations made against adults who work with pupils

1.3 this policy applies to all members of Town Field Primary School (including staff, pupils, volunteers, governors, parents and carers, trainees, community users and visitors)

1.4 This policy is informed by the DfE guidance, including Keeping Children Safe in Education (2018)

2. Monitoring and Review:

2.1 This policy will be reviewed on an annual basis. It is due to be reviewed next in October 2021

2.2 The school will monitor the impact of the policy using:

- Logs of reported incidents
- Monitoring logs of internet activity where appropriate
- Internal monitoring data for network activity
- Pupil, staff and parent questionnaires

3. Roles and Responsibilities

3.1 Governors are responsible for:

- Approving the Online Safety and IT Policy
- Receiving regular information in the form of monitoring reports in regards to online safety incidents and the development of the school's online safety curriculum

3.2 The Headteacher and SLT are responsible for:

- Providing a duty of care for the safety of the school community though the day to day responsibility for online safety will be delegated to a member of staff
- Ensuring that they are made aware of the procedure to be followed in the event of an allegation being made against a member of staff
- Ensure that the member of staff responsible for online safety, the Designated Safeguarding Lead and other relevant staff receive suitable training to enable them to carry out their roles and to train other colleagues
- The Designated Safeguarding Lead is Helena Honeybone

3.3 The Online Safety Lead is Helena Honeybone and is responsible for:

- Working alongside the DSL and the SLT to formulate, implement and evaluate the school's online safety policy
- Providing monitoring and evaluation reports, relating to online safety for the SLT and Governing Body
- Monitoring and reviewing the school's online safety curriculum
- Providing training and updates for all members of the school community to ensure that they are able to fulfil the duties outlined in this policy

3.4 Teachers and support professionals are responsible for:

- Promoting online safety throughout school wherever possible
- Delivering the school's online safety curriculum effectively
- Following the school's safeguarding procedures when dealing with online safety incidents
- Ensuring they undertake training and/or seek guidance to support them in fulfilling their statutory duties

4. Teaching & Learning

Why the internet and digital communication are important:

4.1 The internet is an essential element in 21st century life for education, business and social interaction. The school has a duty to provide pupils with quality internet access as part of their learning experience

4.2 Internet use is a part of the statutory curriculum and a necessary tool for staff and pupils

4.3 Teachers plan internet use carefully to ensure that it is age appropriate and support the learning objectives for specific curriculum areas

4.4 Staff model safe and responsible behaviour in their use of technology during lessons

4.5 Teachers remind pupils about their responsibilities as part of Town Field Primary Acceptable Use Agreement (Appendix 1)

Commented [JJ1]: should this be model ?

Commented [he2R1]: model

Internet use will enhance learning

4.6 The school internet access will be designed expressly for pupil use and will include filtering appropriate to the age of pupils

4.7 Pupils will be taught what internet use is acceptable and what is not and given clear objectives for internet use

4.8 Pupils will be educated in the effective use of the internet in research, including the skills of knowledge location, retrieval and evaluation

4.9 Pupils will be shown how to publish and present information to a wider audience

Pupils will be taught how to evaluate internet content

4.10 The school will ensure that the use of internet derived materials by staff and pupils complies with copyright law

4.11 Pupils will be taught the importance of cross checking information before accepting its accuracy

4.12 Pupils will be taught how to report unpleasant internet content to their class teacher or a member of school staff who will follow safeguarding procedures as necessary and report this to the Online Safety Lead and report the incident to ACS

4.13 The school has a discrete progressive online safety education programme as well as its core messages being interweaved through the school's computing and PSHE schemes. These cover a range of skills and behaviours appropriate to their age and experience, including:

- To develop a range of strategies to evaluate and verify information before accepting its accuracy
- To be aware that the author of a website/page may have a bias or purpose and to develop skills to recognise what that may be
- To know how to narrow down or refine a search
- To understand how search engines work and to understand that this affects the results they see at the top of the listings
- To understand acceptable behaviour when using an online environment/email
- To understand how photographs can be manipulated and how web content can attract the wrong sort of attention
- To understand why online 'friends' may not be who they say they are and to understand why they should be careful in online environments
- To understand why they should not post or share detailed accounts of their personal lives, contact information, daily routines, location, photographs and videos, and to know how to ensure they have turned on privacy settings
- To understand why they must not post pictures or videos of others without their permission
- To know not to downloads any files such as music files without permission
- To have strategies for dealing with receipt of inappropriate materials
- To understand the impact of online bullying, sexting, extremism and trolling and know how to see help if they are affected by any form of online bullying
- To know how to report and abuse, including online bullying and how to seek help if they experience problems when using the internet and related technologies

Online Risks

4.14 The school recognises that pupils increasingly use a range of technology such as mobile phones, tablets, fames consoles and computers. It will support and enable children to use these technologies for entertainment and education but will also teach children that some adults and young people will use such outlets to harm children

Cyber bullying and abuse

4.15 Cyber bullying can be define as 'any form of bullying which takes place online or through smartphones and tablets' (Bullying UK)

4.16 Complaints of online bullying are dealt with in accordance with our Anti-Bullying Policy. Complaints related to child protection are dealt with in accordance with school's child protection procedures

4.17 Through our curriculum pupils are taught to tell a responsible adult if they receive inappropriate, abusive or harmful emails, text messages or messages from other online services such as Whatsapp

4.18 Assemblies, lessons and events provide information about how to get help from Childline, ThinkUKnow and the NSPCC

4.19 Cyber bullying will be treated as seriously as any other form of bullying and will be managed through our anti-bullying procedures. Cyber bullying (along with all other forms of bullying) or any member of the school community will not be tolerated. Full details are set out in the school's policy on anti-bullying and behaviour

Sexual exploitation/sexting

4.20 Sexting between pupils will be managed through our anti-bullying procedures

4.21 All staff are made aware of the indicators of sexual exploitation and all concerns are immediately reported to the DSL

Radicalisation or extremism

4.22 Radicalisation refers to the process by which a person comes to support terrorism and forms of extremism leading to terrorism

4.23 Extremism is defined by the Crown Prosecution Service as 'The demonstration of unacceptable behaviour by using any means or medium to express views which

- Encourage, justify or glorify terrorist violence in furtherance of beliefs
- See to provoke others to terrorist acts
- Encourage other serious criminal activity or seek to provoke others to serious criminal acts
- Foster hatred which might lead to inter-community violence in the UK

4.24 The school understands that here is no such thing as a 'typical extremist'; those who become involved in extremist actions come from a range of backgrounds and experiences and most individuals, even those who hold radical views, do not become involved in violent extremist activity

4.25 The school understands that pupils may become susceptible to radicalisation through online sources as well as a range of social, personal and environmental factors – it is known that violent extremists exploit vulnerabilities in individuals. It is vital that school staff can recognise those vulnerabilities

4.26 Staff will maintain and apply a good understanding of the relevant guidance to prevent pupils from becoming involved in terrorism

4.27 The school will monitor its relevant policies to ensure that they are used to promote community cohesion and tolerance of different faiths and beliefs

4.28 Senior leaders will raise awareness within the school about the safeguarding processes relating to protecting pupils from radicalisation and involvement in terrorism. The school's online safety curriculum overview demonstrates how coverage is closely aligned with the PREVENT agenda as well as the promotion of British values

5. Managing internet access

Information system security:

5.1 School ICT systems security will be reviewed regularly
5.2 Virus protection will be updated regularly
5.3 Security strategies will be discussed with experts such as our IT engineers

Managing Filtering

5.4 Senior staff will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable
5.5 The school will work with their service provider to ensure systems to protect pupils are reviewed and improved
5.6 If staff or pupils discover an unsuitable site, it must be reported to the DSL or Online Safety Lead immediately, as well as ACS as the IT provider being contacted. In their absence, a member of SLT is to be informed

Authorising internet access

5.7 all staff are responsible for adhering to the staff, governor and visitor acceptable use agreement (Appendix 2)
5.8 At EYFS and KS1 access to the internet will be by adult demonstration with directly supervised access to specific, approved online materials
5.9 Any person not directly employed by the school will be asked to sign the staff, governor and visitor acceptable use agreement (Appendix 2) before being allowed to access the internet from the school site

Assessing risks

5.10 the school will take all reasonable precautions to prevent access to inappropriate material however, due to the international scale and linked nature of internet content, it is not possible to guarantee that unsuitable material will never appear on a computer connected to the school network. The school cannot accept liability for any material accessed, or any consequences of internet access
5.11 the school should audit ICT use to establish if the Online Safety and IT Policy is adequate and that the implementation of the Online Safety and IT Policy is appropriate and effective

Handling online safety complaints

5.12 complaints of internet misuse by pupils must be dealt with by a member of SLT.
5.13 Any allegation or disclosure of misuse involving someone who works with children in a paid or voluntary capacity, must be dealt with as per the school's safeguarding and child protection policy
5.14 Complaints that regard safeguarding or child protection nature must be dealt with in accordance with the school's safeguarding and child protection procedure
5.15 Pupils and parents will be informed of the complaints procedure (see school's complaints policy)
5.16 Pupils and parents will be informed of the consequences for pupils misusing the internet

Community use of the internet

5.17 the school will liaise with local organisations to establish a common approach to online safety, if necessary

Email

1.1. Pupils do not have access to email accounts.

1.2. The school:

- Provides staff with an email account for their professional use (Microsoft 365) and makes clear personal email should be through a separate account;
- Does not publish personal email addresses of staff on the school website;
- Will contact the police if one of our staff receives an email that it considers is particularly disturbing or breaks the law;
- Will ensure that email accounts are maintained and up-to-date;
- Reports messages relating to or in support of illegal activities to the relevant authority and, if necessary, to the police;
- Knows that spam, phishing and virus attachments can make emails dangerous.

Published content and the school website

1.3. Staff or pupil personal contact information will not be published. The contact details given online should be for the school office.

1.4. The Head Teacher will take overall editorial responsibility for the school website and social media, ensuring that content is accurate and appropriate, and the quality of presentation is maintained.

1.5. The school website complies with statutory DfE guidelines for publications on its website.

1.6. Most material is the school's own work; where others' work is published or linked to, we credit the sources used and state clearly the author's identity or status.

1.7. The point of contact on the website is the school address and telephone number. The school uses a general email contact address: admin@woodfield.doncaster.sch.uk

1.8. Photographs published on the web do not have full names attached.

1.9. The school's Twitter page is subject to the same expectations as the school website.

Publishing pupils' images and work

1.1. Pupil image file names will not refer to the pupil by name.

1.2. The school gains parental permission for use of digital photographs or video involving their child by using The Rose Learning Trust's Images and Videos Parent Consent Form to gain written permission.

Managing videoconferencing and webcam use

1.10. Videoconferencing and webcam use, if used as part of a lesson, must be approved by the Online Safety Lead and will be appropriately supervised.

Managing emerging technologies

1.11. Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed.

1.12. The SLT should note that technologies, such as mobile phones with wireless internet access, can bypass school filtering systems and present a new route to undesirable material and communications.

1.13. Mobile phones will not be used during school time unless express permission has been granted by the Head Teacher. Pupils' requiring emergency mobile phones must be stored in the office during the school day and written parental consent gained.

Commented [JJ3]: Is this anybody i.e. all staff or is it referring to just pupils

Commented [he4R3]: children

Protecting personal data

1.14. Personal data will be recorded, processed, transferred and made available according to the school's GDPR policy and the Data Protection Act 2018.

Commented [JJ5]: should be school at least for the time being.

2. Mobile Devices (including mobile phones)

Personal Devices

2.1. The recording, taking and sharing of images, video and audio on any mobile phone is not permitted by any staff or visitors, except where it has been explicitly agreed otherwise by the Head Teacher.

2.2. Where parents or pupils need to contact each other during the school day, they should do so only through the school's telephone. Staff may use their phones during break times. If a staff member is expecting an urgent personal call, they need to seek specific permission from the Head Teacher to use their phone at times other than their break times.

2.3. Mobile phones and personally-owned devices will not be used in any way during lessons. They should be switched off or on silent at all times.

Commented [JJ6]: Totally agree with 2.2 and 2.3 but how well do staff understand this ?

2.4. Mobile phones and personally-owned mobile devices brought in to school are the responsibility of the device owner. The school accepts no responsibility for the loss, theft or

damage of personally-owned mobile phones or mobile devices.

2.5. Staff are not permitted to use their own mobile phones or devices for contacting children, young people or their families within or outside of the setting in a professional capacity unless in the case of an emergency, out of school hours or express permission has been granted by the Head Teacher.

2.6. Staff must use the school phone where contact with pupils' parents is required.

2.7. If a member of staff breaches the school policy, disciplinary action may be taken.

2.8. Where staff members are required to use a mobile phone for school duties, for instance in case of emergency during off-site activities, or for contacting pupils or parents the following guidance should be adhered to. In an emergency where a staff member doesn't have access to a school- owned device, they should use their own device and hide (by inputting 141) their own mobile number for confidentiality purposes.

Commented [JJ7]: this sentence is not complete.

2.9. Pupils will abide by the following rules when using personal devices in school:

- The school strongly advises that pupil mobile phones should not be brought into school; however, we accept that there may be circumstances in which a parent wishes their child to carry a mobile phone to/from school for their own safety. In this case, it must be stored in the school office and collected at the end of the school day. A parental consent form must also be completed.
- Pupils should protect their phone numbers by only giving them to trusted friends and family members. Pupils will be instructed in the safe and appropriate use of mobile phones and personally-owned devices and will be made aware of boundaries and consequences.

Work Devices

2.10. Staff agree to the conditions set out in the Device User Agreement (Appendix 3) in regards to using devices provided by the school.

2.11. Staff should only use work devices (e.g. laptop, iPad, etc.) for business use.

2.12. Staff in charge of school devices are responsible for their care and security. All reasonable measures should be taken to ensure the correct care of the device and to ensure it is kept secure both on- and off-site. The school may charge staff for repairs or replacement of technology where misuse or carelessness was the cause of damage.

2.13. Where staff make recordings (i.e. image, audio, video, etc.) of pupils using school devices, they are responsible for deleting those recordings once they have been transferred to the relevant medium.

2.14. All school devices which hold school-related data and recordings must be password protected / stored securely within the school premises or securely at home. When in

transit in a vehicle, devices must be stored in a locked boot to meet insurance guidelines.

2.15. Staff are responsible for ensuring they follow the school's GDPR and Data Protection policies in regards to processing data on their work devices.

2.16. In line with the school's Staff, Governor and Visitor Acceptable Use Policy, staff should not download or stream from sources whose security is questionable in any way or for uses which are not school related. If in any doubt about security of a website, staff should refer to the ICT Technician before attempting download.

2.17. Staff are responsible for ensuring they act in accordance with copyright laws when copying or downloading for work or other purposes.

3. Social networking and personal publishing

3.1. 'Social media' is the term commonly given to websites and online tools which allows users to interact with each other in some way by sharing information, opinions, knowledge and interests. As the name implies, social media involves the building of communities or networks, encouraging participation and engagement. This may, for example, include Facebook, Twitter, Instagram, YouTube.

3.2. All staff must exercise professional judgement when using social media for both business and personal use.

3.3. Employees are personally responsible for the content they publish on social media both at work and outside of work using either school or personal equipment. Employees therefore must assume that any comments may be visible to anyone in the world with an internet connection and are a permanent record and can be republished in other media.

3.4. The public must be able to trust the integrity of the school. They need to be confident that the outside activities of employees do not undermine the school's reputation and that decisions regarding school matters are not perceived to be influenced by an employee's commercial, political or personal interests.

3.5. All staff should bear in mind that any information or images they share through social networking applications, even if they are on private spaces, are still subject to relevant legislation, including: copyright, data protection, Freedom of Information and the staff code of conduct.

3.6. Town Field Primary School has established a Twitter account. The management of these accounts and the creation of new social media accounts is the responsibility of the Business Manager and Head Teacher.

3.7. Staff, when using social media for both personal and professional use, must therefore:

- conduct themselves in an honest and professional manner;
- ensure that their conduct and activities do not bring the school into disrepute;
- use their professional judgement when expressing views in order to avoid any reputational damage to the school;
- be mindful of how their private interests may impact on their duty to the school and therefore not put themselves in a position where their duty and private interests conflict or appear to conflict;
- not breach Data Protection or confidentiality by talking about, identifying or disclosing personally identifiable information about parents, pupils or colleagues;
- not post comments or photos which may be deemed offensive;
- not use official school logos on personal web pages;
- not use personal email accounts or mobile phones to make contact with members of the school community on school business, nor should any contact be accepted;
- not use a school e-mail address to register on social media sites for personal use;
- not place personal postings on social media sites using their own personal mobile or device during normal working time;
- not invite or accept new 'friend' requests on Facebook on their personal profile if they are aware they are parents, or pupils (current or former), from the school community unless there is a previously established personal relationship;
- not link themselves to Town Field Primary School or The Rose Learning Trust on personal accounts.

3.8. Town Field recognises the potential of social media to support the professional development of our staff. When using social media for educational and professional development purposes are encouraged to observe the following practices:

- employees should set up a distinct and dedicated social media site or account for educational purposes and this must be separate from any personal social media;
- the content of this site should be wholly professional and must not bring the school into disrepute;
- care must be taken that any links to external sites from any professional accounts are appropriate and safe.

4. Communications policy

Introducing the Online Safety Policy to pupils

4.1. The school's Digital Code of Conduct and Pupil Acceptable Use policy (Appendix 1) is discussed with pupils regularly through assemblies and lessons.

4.2. Pupils will be informed that network and internet use will be monitored and appropriately followed up.

4.3. The school's programme of training in Online Safety will be reviewed by the Online Safety Leads, PSHE Lead and DSL.

Staff and the Online Safety policy

4.4. All staff will be given the school Online Safety Policy which they will sign for and have its importance explained.

4.5. Staff adhere to the Staff, Governor and Visitor Acceptable Use Policy (Appendix 2).

4.6. Staff must be informed that network and internet traffic can be monitored and traced to the individual user.

4.7. Staff that manage filtering systems or monitor ICT use will be supervised by senior management and work to clear procedures for reporting issues.

Enlisting parents' support

4.8. Parents' attention will be drawn to the School Online Safety and IT Policy and associated material on the school website.

4.9. The Online Safety Lead on behalf of the school will maintain a list of online safety resources for parents and make this available on the school's website.

Commented [JJ8]: suggest we add this otherwise parents will be unaware of the resource

Appendix 1 – Pupil Acceptable Use Agreement

Pupil Acceptable Use Agreement

Ready

- I am aware that some websites and social networks have age restrictions and that I should respect this.
- I will only use the school's computers for school work and homework.
- I understand that there are consequences for negative online behaviours – whether conducted inside or outside of school.
- I will not open an attachment, or download a file, unless I know and trust the person who has sent it.
- If I see anything I am unhappy with, either for myself or my peers, or if I receive a message that I do not like, I will not respond to it but I will report to a teacher / responsible adult.

Respectful

- I will only edit or delete my own files and not look at, or change, other people's files without their permission.
- I will not bring files into the school without permission or upload inappropriate material to my workspace.
- I understand that any personal technological devices which I bring to school are (a) my own responsibility (b) required to be held securely by the school until the end of the day (c) not allowed to be used for recording within school in any way. I will not use mobile phones to send inappropriate communication, photographs or videos.
- The messages I send, or the information I upload, will always be polite and respectful.

Safe

- I understand that network and Internet use is monitored.
- I will not attempt to visit Internet sites or conduct online searches that I know to be banned by the school.
- I will keep my logins and passwords secret.
- I will not give my home address, phone number, send a photograph or video, or give any other personal information that could be used to identify me, my family or my friends, unless a trusted adult has given permission. I will never arrange to meet someone I have only ever previously met on the Internet, unless my parent/carer has given me permission and I take a responsible adult with me.

Appendix 2 – Staff, Governor and Visitor Acceptable Use Agreement

Staff, Governor and Visitor Acceptable Use Agreement

Whilst our school promotes the use of technology, and understands the positive effects itcan have on enhancing pupils' learning and community engagement, we must also ensure that staff use technology appropriately.

This acceptable use agreement is designed to outline staff responsibilities when using technology, whether this is via personal devices or school devices, or on/off the school premises, and applies to all staff, volunteers, contractors and visitors.

1. **Using technology in school**

- I will only use ICT systems, such as computers (including laptops) and tablets, which have been permitted for my use.
- I will only use the approved email accounts that have been provided to me.
- I will not use personal emails to send and receive personal data or information.
- I will ensure that any personal data is stored in line with the GDPR.
- I will delete any chain letters, spam and other emails from unknown sources without opening them.
- I will only use the internet for personal use during out-of-school hours, including break and lunch times.
- I will not search for, view, download, upload or transmit any suspicious, explicit or inappropriate material when using the internet.
- I will not share school-related passwords with pupils, staff or third parties unless permission has been given for me to do so.
- I will not download or install any software onto school ICT systems unless instructed to do so by the Online Safety Lead or IT Technician.
- I will ensure any school-owned device is protected by anti-virus software and that I check this on a termly basis.

2. **Mobile devices**

- I will only use personal mobile devices during out-of-school hours, including break and lunch times, unless expression permission has been granted by the Head Teacher.

- I will ensure that mobile devices are either switched off or set to silent mode during school hours, and will only make or receive calls in specific areas, e.g. the staffroom.
- I will ensure mobile devices are stored securely.
- I will not use mobile devices to send inappropriate messages, images or recordings.
- I will ensure that personal and school-owned mobile devices do not contain any inappropriate or illegal content.
- I will not access the Wi-Fi system using personal mobile devices.
- I will not use personal and school-owned mobile devices to communicate with pupils or parents except ~~,~~in cases of emergency.
- I will not take or store any images or videos of pupils, staff or parents on any mobile device unless consent has been sought from the individual(s) in the images or videos or. Only pupils with parental consent may have their image or video taken.
- In line with the above, I will only process images or videos of pupils, staff or parents for the activities for which consent has been sought.

Commented [JJ9]: suggested added wording to make compatible with policy

3. Social media and online professionalism

- If I am representing the school online, e.g. through blogging or on school social media account, I will express neutral opinions and will not disclose any confidential information regarding the school, or any information that may affect its reputability.
- I will not use any school-owned mobile devices to access personal social networking sites.
- I will not communicate with pupils or parents over personal social networking sites.
- I will not accept 'friend requests' from any pupils or parents over personal social networking sites
- I will ensure that I apply the necessary privacy settings to any social networking sites.
- I will not publish any comments or posts about the school on any social networking sites which may affect the school's reputability.
- I will not post or upload any defamatory, objectionable, copyright infringing or private material, including images and videos of pupils, staff or parents, on any online website.
- I will not give my home address, phone number, mobile number, social networking details or email addresses to pupils or parents – any contact with parents will be done through authorised school contact channels.

4. Working at home

- I will adhere to the principles of the GDPR when taking work home.

5. Training

- I will ensure I participate in any e-safety or online training offered to me, and will remain up-to-date with current developments in social media and the internet as a whole.
- I will ensure that I allow the Online Safety Lead and DPO to undertake regular audits to identify any areas of need I may have in relation to training.
- I will ensure I employ methods of good practice and act as a role model for pupils when using the internet and other digital devices.
- I will ensure that I deliver any training to pupils as required.

6. Reporting misuse

- I will ensure that I adhere to any responsibility I have for monitoring, as outlined in the Online Safety policy e.g. to monitor pupils' internet usage.
- I will ensure that I report any misuse by pupils is reported to a member of the Senior Leadership Team.
- I will ensure that I report any misuse by staff members breaching the procedures outlined in this agreement in accordance with the school's safeguarding procedures.
- I understand that my use of the internet will be monitored and recognise the consequences if I breach the terms of this agreement.
- I understand that the school may decide to take disciplinary action against me if I breach this agreement.

Signed:_____ Date: _____

PRINT NAME: _____

Appendix 3 – Device User Agreement

Device User Agreement

Town Field Primary School has created this agreement to ensure that staff understand their responsibilities when using school-owned devices, such as iPads, laptops etc whether on or off the school premises.

The school

Town Field Primary School retains sole right of possession of any school-owned device and may transfer the device to another staff member if you do not, or are unable to, for any reason, fulfil the requirements of this agreement.

Under this agreement, the school will:

- If it is a requirement of your role, provide devices for your sole use while you are a permanent full-time or part-time employee at the school.
- Ensure devices are set up to enable you to connect to, and make effective use of, the school network.
- Ensure the relevant persons, such as the IT Technician, have installed the necessary security measures on any school-owned device before your use – including, but not limited to, the following:
  - Firewalls
  - Malware protection
  - User privileges
  - Filtering systems
  - Password protection and encryption
  - Mail security technology
  - Tracking technology
- Ensure that all devices undergo regular checks and updates.
- Plan and manage the integration of devices into the school environment, and provide the professional development required to enable you to use the devices safely and effectively.
- When required, expect you to pay an excess for accidental damage or loss repair/replacement costs, where loss or damage is a result of your own negligence.

Under this agreement, you will:

Overall use and care

- Transport the device safely.
- Not permit any other individual to use the device without your supervision.
- Take responsibility for any other individual using the device.
- Provide suitable care for the device at all times and not do anything that would permanently alter it in any way.
- Lock the device screen when not in use with a passcode.
- Keep the device clean.
- Securely store devices.
- Ensure all devices are switched off or set to silent mode during school hours.
- Immediately report any damage or loss of the device to the Business Manager.
- Ensure any tracking technology applied is active at all times.
- Immediately report any viruses or reduced functionality following a download or access to a site, to the Online Safety Lead and make contact with ACS.
- Be prepared to cover the cost for repair or replacement of the device when the damage or loss has been a result of your own negligence.
- Make arrangements for the return of the device and passcode to the Business Manager if your employment ends or if you will be away from the school for a long period of time.

Using devices

- Only use the devices that have been permitted for your use.
- Only use devices for educational purposes.
- Only use apps that are GDPR-compliant and from reputable sources.
- Ensure that any personal data is stored in line with the GDPR.
- Give permission for the IT Technician to erase and wipe data off your device if it is lost, or as part of exit procedures.
- Obtain permission prior to accessing learning materials from unapproved sources.
- Not search for, view, download, upload or transmit any explicit or inappropriate material when using the internet.
- Not share any passwords with pupils, staff or third parties.
- Ensure your device is protected by anti-virus software installed by the IT Technician and that this is checked on a termly basis.
- Not use your device to send any inappropriate messages, images or recordings.
- Ensure that your device does not contain inappropriate or illegal content.

Failure to agree to, or abide by, these terms will lead to the device being returned to the school and serious breaches may result in disciplinary action.

Signed:_____ Date: _____

PRINT NAME:

1.3. The school does not identify pupils using their full name in online photographic materials or include the full names of pupils in the credits of any published school produced video materials/DVDs.

1.4. Pupils are advised to be very careful about placing any personal photos on any 'social' online network space. They are taught to understand the need to maintain privacy settings so as not to make public, personal information.

Pupils are taught that they should not post images or videos of others without their permission. The school teaches them about the risks associated with providing information with images (including the name of the file), that reveals the identity of others and their location, such as house number, street name or school. The school teaches them about the need to keep their data secure and what to do if they are subject to bullying or abuse.